

Description

[Electronic Files Digital Rights Management.]

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] US Patent Documents 5425029 Jun., 1995 Hluchyj et al. 370/235. 5568487 Oct., 1996 Sitbon et al. 709/230. 5682534 Oct., 1997 Kapoor et al. 709/203. 5727002 Mar., 1998 Miller et al. 709/237. 5822524 Oct., 1998 Chen et al. 709/203. 5854841 Dec., 1998 Nakata et al. 709/203. 5889954 Mar., 1999 Gessel et al. 709/223. 5903724 May., 1999 Takamoto et al. 709/200. 6021440 Feb., 2000 Post et al. 709/231. 6046979 Apr., 2000 Bauman 370/229. 6061796 May., 2000 Chen et al. 709/225. 6269467 Jul., 2001 Chang et al. 716/1. 6519636 Feb., 2003 Engel et al. 709/223.

BACKGROUND OF INVENTION

[0002] Illegal distribution and transfer of copyrighted digital audio, video, picture, and document content online is a huge problem especially to the commercial businesses that are

most affected by theft/unauthorized duplication, replication, or transfer of said content. This invention makes it possible to significantly reduce the illegal distribution of stolen music, video, audio, picture and documents over the Internet, electronic networks or computer systems.

[0003] Every digital file has a unique hash. Thus, a song mastered on a CD that is then copied illegally and transferred over the Internet has a unique hash "fingerprint" from the same song if copied legally for legitimate purposes. By creating a database of illegally copied music it is possible to use the unique hash fingerprints of each music file to help identify music, which is being illegally copied and distributed. It is important to note that music legally purchased over the Internet has a different hash "Fingerprint" than that copied illegally. Understanding this now makes it possible to identify music files that have been illegally copied and transferred via the Internet. Similarly, creating databases of stolen picture, video, audio or other documents together with their associated hash "Fingerprints" also makes it possible to identify illegal transfer and use of these files.

[0004] The hash fingerprints have been used in court cases as a way to prove that one file was identical to another file that

was an illegal copy. This invention recognizes that there is a better and earlier way to identify the illegally copied content sooner and stop it before the damaging effects of digital theft could be realized. It also became clear that the only way to effectively combat the rising costs of stolen content would be to create a system, method, and apparatus that could work effectively and efficiently at a network level and computer system level. One such approach is to have a specific method that could have the network communicate with the operating system and operating system communicate with specific applications to identify stolen content that is being transferred over the Internet. Once identified the illegal distribution would be stopped dynamically from completing the transfer. This same approach could be used to prevent illegally copied files from being executed on computer systems and other digital devices such as digital audio players like Apple Computer's iPod or Diamond MultiMedia S3's Rio or even digital hard disc recorders and digital disk recorders.

[0005] One problem that became clear was that once content was recognized, there was no way to allow a user to legitimize the content they had previously downloaded or were in the process of downloading. One such way could be to al-

low them to purchase the content at an online music store or to purchase it directly on their computer system whereby their copy of the illegal distribution could be re-encoded and serialized or otherwise encrypted to match the new owner of the copy after a purchase. Another option might be, in the case of documentation, to prompt the user to ask for permission to open a document that they are not authorized to open.

[0006] Positive identification, in the form of using a digital fingerprint, such as a hash (Md5, Md2, SHA-1, etc), of files while in transit has not been addressed by any of the prior art. The recent speed increases of processors in firewalls, IDS (Intrusion Detection Systems), and IPS (Intrusion Prevention Systems) has only recently made it possible to implement such a system without slowing down the transmission of information while performing such a task on a network appliance.

[0007] In addition, no prior art exists in this space partly because there was no mechanism for owners of digital information to identify a specific file rather than a specific file type or document data in a way that was conclusive and could be court accepted. Now hash signatures such as MD5 have been used in court cases and are proven methods of iden-

tification and no prior art takes into account a mechanism for using these fingerprints to identify files in transit or files in the process of being executed and perform an action based on that data.

[0008] The RIAA has used hash fingerprints in a database that contains only those fingerprints for identification purposes of stolen audio content such as Mp3s. The process used is not automatic and not scalable or usable on a corporate network or by an operating system or user application. Also, the RIAs process does not take into account other types of digital content such as video, documents, or pictures.

SUMMARY OF INVENTION

[0009] This invention relates to the field of identifying and controlling digital data such as digital audio, digital video, and digital documents such as one or more of the following: mp2, mp3, mp4, AAC, dv, MPEG1, MPEG2, MPEG3, MPEG4, JPEG, TIFF, GIF, .doc, .ppt, .xls and others sent to and received from a computer system or application connected to a network, particularly over one or more of the following: the internet, intranet, cable, wireless and any other of packet switching networks.

[0010] More specifically, the invention relates to a way to control

how data is communicated to an application on the network and how packets received from the network are passed to the application and how an operating system identifies and controls, through an application, the use of the data through a series of checks and balances and a bi-directional rule set containing hash values or fingerprints of each file as identified by ourselves or our potential partners such as the RIAA or ASCAP or other media control organizations that work on behalf of the record or video industry. This invention also relates to how the digital data is transmitted over the network by storing the application providing the hash database of stolen audio or video data on a firewall application whereby the files are checked in transit to verify that they are not stolen and therefore can be passed; if they are stolen, the download or upload is stopped in transit and other options may be presented to the user at that time. If the file is executed on a computer system, the user may be asked to purchase the music from an online music store or to legitimize the copy contained on their computer wherein the song is re-encoded at a charge to the user on the user computer system.

BRIEF DESCRIPTION OF DRAWINGS

- [0011] FIG. 1 is a functional block diagram of the method of computing a file hash signature and comparing it to a database of known file signatures; and
- [0012] FIG. 2 is a functional block diagram of a computer system in which is installed digital content distribution control software; and
- [0013] FIG. 3 is a flow chart illustrating the method of operation of the system of FIG. 2; and
- [0014] FIG. 4 is a flow chart illustrating the method of one operation of the system of FIG 3; and
- [0015] FIG. 5 is a flow chart illustrating the method of one operation of the system of FIG 3; and
- [0016] FIG. 6 is a flow chart illustrating the method of one operation of the system of FIG 4.

DETAILED DESCRIPTION

- [0017] For the purpose of illustration, the following example is described with reference to the Apple Macintosh OS X.TM. series of operating systems, although it will be appreciated that the invention is also applicable to other operating systems including Microsoft Windows.TM. Series operating systems, Apple Macintosh 9 systems, Linux, Unix, SCO, BSD, FreeBSD, Microsoft Windows CE.TM., Microsoft Windows NT.TM., Microsoft Windows XP.TM., IBM AIX and

OS/2.

[0018] With reference to FIG. 1, a method contained inside of a computer system is described as containing a file 1 that is being interrogated by a file comparator process 2 via an electronic link 6 to compute a hash signature and compare said signature to those contained in a database containing digital content file signatures 4. The logical link 7 connecting the two processes and the file comparator 2 returning a result 3 of MATCH or NO MATCH.

[0019] With reference to FIG. 2, an end user computer 1 has a display 2 and a keyboard 3. The computer 1 additionally has a processing unit and a memory which provide (in functional terms) a graphical user interface layer 4 which provides data to the display 2 and receives data from the keyboard 3. The graphical user interface layer 4 is able to communicate with other computers via a network interface 5 and a network 6. A network manager 7 controls the network.

[0020] Beneath the graphical user interface layer 4, the CPU runs a number of user applications. In FIG. 2, only a single application 8 is illustrated and may be, for example, Apple iTunes.TM. The application 8 communicates with a file system 9, which forms part of the Apple Macintosh OS

X.TM. Operating System and which is arranged to handle file access requests generated by the application 8. These access requests include file open requests, file save requests, file copy requests, etc. The lowermost layer of the operating system is the disk controller driver 10, which communicates with and controls the computer's hard disk drive 11. The disk controller driver 10 also forms part of the Apple Macintosh OS X.TM. Operating System.

[0021] Located between the file system 9 and the disk controller driver 10 is a file system driver 12, which intercepts file system events generated by the file system 9. The role of the file system driver 12 is to co-ordinate digital content operations for data being written to, or read from, the hard disk drive 11. In dependence upon certain screening operations to be described below, the file system driver 12 enables file system events to proceed normally or prevents file system events and issues appropriate alert messages to the file system 9.

[0022] The file system driver 12 is functionally connected to an ACE (Analytic Control Engine) controller 13, such that file system events received by the file system driver 12 are relayed to the ACE controller 13. The ACE controller is associated with a database 14 which contain a set of "signa-

tures" previously determined for respective digital files. For the purposes of this example, the signature used is a checksum derived using a suitable checksum calculation algorithm, such as the US Department of Defense Secure Hash Algorithm (SHA, SHA-1, SHA-224), MD5, MD2, or the older CRC 32 algorithm or other open source or proprietary algorithm capable of generating a hash signature value deemed acceptable to determine that one file is an identical copy of another file.

[0023] The database 14 contains a set of signatures derived for known digital content. Updates may be provided by way of floppy disks, CD, DVD, flash drive, FireWire, USB, or directly by downloading them from a remote server 17 connected to the Internet 18.

[0024] Only the network manager 7 and/or authorized computer administrator has the authority to modify this database 14 using signatures of digital content such as MP3, MP4, AAC, JPEG, GIF, TIFF, MPEG, DVD, etc.

[0025] Upon receipt of a file system event, the ACE controller 13 first analyses the file associated with the event (and which is intended to be written to the hard disk drive 11, read, copied, etc) to determine if the file matches that of a file identified to match content in the database 14.

[0026] The ACE controller 13 scans the database 14 to determine whether or not the corresponding signature is present in that database 14. If the signature is found there, the ACE controller 13 reports this to the file system driver 12. The file system driver 12 in turn causes the system event to be suspended and causes an alert to be displayed to the user that known digital content was found. The file system driver 12 may also cause a report to be sent to the network manager 7 via the local network 6. The file system driver 12 quarantines the infected file on the hard disk drive 11.

[0027] The file scanning system described above is further illustrated by reference to the flow chart of FIG. 3.

[0028] It will be appreciated by the person of skill in the art that various modifications may be made to the embodiment described above without departing from the scope of the present invention. For example, the file system driver 12 may make use of further digital content controllers including controllers arranged to screen files for illegitimately copied digital content other than hash identifiable. The file system driver 12 may also employ re-encoding systems data encryption systems.

[0029] It will also be appreciated that the file system driver 12

typically receives all file access traffic, and not only that relating to hard disk access. All access requests may be passed to the ACE controller 13 which may select only hard disk access requests for further processing or may also process other requests relating to, but not limited to, floppy disk data transfers, network data transfers, DVD, DVD-R, DVD-RW, CDROM, CD-RW, CD-R data transfers, USB, USB 2.0, FireWire, FireWire 2, and associated peripheral flash storage devices.

[0030] It will also be appreciated that the file system driver 12 and file system 9 along with applications 8 and GUI 4 can be those related to hand held, cell phone, PDA, digital camera, digital storage, or other devices containing a method to process electronic data as described above. It is also appreciated that hard disk drive 11 can be any electronic storage device such as flash, FireWire IEEE 1394, USB, USB 2.0, FireWire 2.0, and other electronic storage devices such as SD, MD, CF, etc. It is also appreciated that keyboard 3 can be any input device such as a cell phone keypad, microphone, or other electronic interface to a computer system or electronic device via wired or wireless connection.

[0031] With reference to FIG. 4, a flow chart of the process illus-

trated in FIG 3 "INTERRUPT EVENT AND SET ALERTS AND NOTIFICATIONS" is shown. The database referenced in FIG. 4 is the same database as referenced in claim 1 wherein one field in the said database contains alert and notification parameters.

[0032] With reference to FIG. 5, a flow chart of the process illustrated in FIG 3 "SET FILE AND DATABASE ACTIONS" is shown. The database referenced in FIG. 3 is the same database as referenced in claim 1 wherein one field in the said database contains file and database action parameters.

[0033] With reference to FIG. 6, a flow chart of the process illustrated in FIG 4 "DISPLAY OPTIONS" is shown. The options shown are outlined in detail as they may be presented to a user of a computer system or other electronic device. This illustration is shown as one embodiment of options that may be presented; it does not outline every possible option as a network manager or remote system may define other options. These options will be presented in the database as claimed in claim 1 and said database will pass these parameters to the function in software.